INTELLIGENCE

EU Companies and Cybersecurity Threats

Published 3 years ago on January 2, 2020
By Dr.Luciano Magaldi

PUBLICATIONS

Companies must be the protagonists in the fight against cybercrime through the synergic application of different skills and disciplines, in the perspective of tackling complex phenomena such as cybercrime.

There are many and challenges that the **EU companies**, in a globalized economy, in the face of modern digital development, are called to face – they must be personally involved in the prevention, emergence and containment of the effects of cyber-attacks.

A company must be appropriately adequate to the level of concrete risks for the conduct of its activities, in order to make possible and facilitate the exercise of public functions of monitoring and ascertaining wrongdoing activities.

The Numbers of Cybercrime

The issue of the relationship between cybersecurity and companies is increasingly significant, and this report is now central by going hand in hand with the development of digital technologies and their use, not only for economic growth and development, but also for criminal purposes.

At the same time, many cyber-events precisely confirmed that the essential use of IT tools in the management of business activities – and are market players – are particularly vulnerable and exposed to cyber-attacks, as evidenced by the data processed by **IOCTA – the Internet Organized Crime Threat Assessment** – prepared annually by the **European Cyber Center (EC3), which operates within Europol**.

Only in 2017 the **WannaCry** and **Notpetya** attacks, consisting of the **spread of 300,000 users' data** worldwide, in more than 150 countries, with economic damage of around 4 billion dollars.

The **World Economic Forum**, which, in its **2019 Global Risk Report**, ranked cyberattacks among the top five global risks.

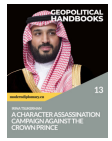
The Close Connection Between Computer Security and Personal Data Protection

All that is indicative of the need for an effective, innovative and integrated approach to the problem of fighting cybercrime, based on active corporate involvement and fruitful

Armenia's Existential Threats and Strategic Issues

Rethinking Iran: 1979-2019

A character assassination campaign against the Crown Prince



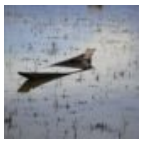
LATEST

ENVIRONMENT / 2 hours ago

For Somalia, nature is key to lasting peace

RUSSIA / 4 hours ago

Mikhail Bogdanov's Passion for Africa and the Critical Russia's Policy Debates -Part 1



FINANCE / 7 hours ago

$500M World Bank Financing to Help Bangladesh Improve Disaster Preparedness

REPORTS / 9 hours ago

Reforms Can Support Inclusive Growth in Turbulent Economic Times

collaboration between the public and private sectors.

It is no longer possible to react without an integration of technical-scientific, legal and economic expertise to ensure the development of appropriate cybersecurity systems in order to protect the confidentiality of data, by including the prevention, containment and management of cyber-risks.

This trend has begun to develop over the last twenty years – we have seen the emergence of new safety control systems in EU companies who have to facilitate the sharing of good practices.

From a legal point of view, the focus is on finding effective ways of protecting against illegal activities that can jeopardize the confidentiality of information stored by companies, causing considerable capital damage.

The Need for Supranational Regulation

The need for a uniform regulation of the subject in the supranational field is based on the adoption of European Union legislation, i.e. with the adoption of GDPR to protect the treatment and free movement of personal data.

This goal gives private market entities a central role in fighting cyber-attacks and protecting the confidentiality of personal data from the same threats, as well as the massive amount of information of employees, agents, associates and suppliers that companies possess.

New Organization and Control Obligations for Companies

The imposition of new obligations on companies about cyberthreats against their organizations and control, as well as notifications to the relevant authorities, aim to make private entities accountable and aware by promoting the spread of a culture of cyber-security, capable of developing virtuous synergies with the functions of public authorities.

By implementing an effective circulation of information, that will achieve an acceptable level of containment and risk management in a globalised economy environment.

Information Circulation, Exchange and Development of Best Practices

FINANCE / 14 hours ago

Poland's Growth Potential Could Reach 4 Percent with Reforms and Investments

WORLD NEWS / 16 hours ago

CFP: IV Eurasian Research on Modern China and Eurasia Conference

AMERICAS / 18 hours ago

China's vision of the results and outputs of the Jeddah summit and the American role

A central importance is given to the breach notification system prepared by the current EU regulations that provide for a timely communication of the incident that affected the continuity and/or provision of the service.

The logic of public-private partnership serves not only in the preparation of prevention and risk control procedures but also for an information exchange system with companies – in fact, the relevance of this mechanism of rapid transmission of news and immediate intervention is expressed with the possibility of reporting a different subject, compared to the recipients of the legislation.

The prospect of information circulation, exchange and development of best practices is also enhanced in the supranational field, as required by the current cross-border survey of economic activities, with the dissemination and processing of data, as well as cybercrime itself.

The configuration of a network of bodies from different countries belonging to the European Union in order to achieve a fruitful form of cooperation in the exercise of their respective powers will be a single point of contact for facilitating effective contacts between the relevant public authorities within the European Union and international authorities.

Non-EU Data Protections

All of this has been mentioned before, including companies in borders beyond the European Union, provided that the owner or controller is established within the European Union, a testament to the global dimension of the phenomenon: the necessary appropriate organisational and technical measures to protect the integrity and confidentiality of data is essential for the EU recipients of the legislation.

It also enhances the provision by the private sector of good practices and guidelines, stipulating that compliance of the treatment to the current legislation can be provided by adhering to codes of conduct drawn up by associations of category, as well as by obtaining ad hoc certifications.

The Function of the Data Protection Officer (DPO)

EU companies, in the near future, a must operate with forms of risk assessment in practice and with preparation of the organizational measures, extended to all stages of the processes of management of confidential information and evaluation of the real effectiveness of the carried measures.

The provision of an additional monitoring body is represented by the **DPO – Data Protection Officer** – with the important function of raising awareness of those involved in the exercise of activities at risk – he will train the company's staff and will be a contact and control exchange with national authorities.

DPO can be tied with solutions tested in other areas where models have been tested and based on the independent provision of rules in a broad sense of caution with the exercise of effective internal controls, as well as on the enhancement of virtuous practices and acts of soft law.

Access and Cooperation in Digital Evidence

It is a role that works in the field of investigation and research of evidence, especially when accessing **digital evidence**: forms of direct cooperation between public authorities and service providers of other countries are contemplated in recent regulatory proposals drawn up within the European Union and the African Union.

Such measures would be carried out in the absence of mediation by the public authority of the reference country, and it must be align with the requirements of speed/effectiveness of computer investigations.

It is also a matter of using cooperation tools that reflect the new needs of research and the acquisition of volatile and virtual evidence, which need to be insured and protected quickly – small companies included, will have to become prominent players in the fight against cybercrime through the synergic application of different skills and disciplines in the perspective of tackling complex phenomena such as cybercrime.

Share this:







RELATED TOPICS: #BUSINESS #CYBERSECURITY #EUROPEAN UNION

DON'T MISS

The World in 2020

UP NEXT

Beijing's Export of Surveillance Technology

Dr.Luciano Magaldi

Dr. Luciano Magaldi Orta Nova, after his PhD in Cloud Computing at Cloud Universityby Rackspace in San Antonio, Texas, a Master of Science in Security Engineeering at Cibrary Faculty of Washington, the Tesol certificate at Arizona State University in Tempe, a Bachelor of arts in Interpreting and Translating at Lus Pio V in Rome, an SEO specialization at the University of California Davis (UC Davis), a DSA specialisation at the University of London, an ETL specialisation at the Universitat Aut'onoma of Barcelona, an academic diploma in Forensic Sciences at Oxford Royale Academy, a specialising certificate in American Politics at Harvard Kennedy School, a professional certificate in mathematics at Stanford University, a Copyright Law certificate at MIT in Cambridge, used to work for Google Ireland in Dublin, Apple European campus in Cork, Ireland, and Amazon Slovakia in Bratislava. Dr. Luciano Magaldi finally obtained his specialisation in journalism at Michigan State University School of Journalism. His career as a journalist began writing articles for AgoraVox France and AgoraVox Italia about world politics, military issues and cyber-tech.

YOU MAY LIKE

Business on Instagram: the secrets

Double standards haunt US and Europe in dealings with Turkey and the Middle East

Genesis, Institutions and Instruments of the EU: A Concise Guide on Euro-Multilateralism

What Would Happen to Russia Without the United States and Europe?

Space – the greener frontier – is good for business

Geopolitics or "Pegasus Case": What Stops Dialogue between Madrid and Catalonia

COMMENTS

INTELLIGENCE

China and the CIA Project of right Judgments of Future Predictors

Published 23 hours ago on July 18, 2022
By **Dr.Nadia Helmy**

The (Project of Sound Judgments of Brilliant Future Predictors), which is funded by the "Advance Intelligence Research Projects Activity" section of the US government and the US Central Intelligence Agency (CIA), is striving to recruit, sort and employ brilliant geniuses who are able to predict the future in an unprecedented and genius way, by discovering new ways in advanced intelligence proactive thinking, which allows predicting the shape of the future and the new world order, and its network of international alliances globally

Here, the Central Intelligence Agency (CIA's accurate and right Judgments of the Future Predictors Project) believes that there are real geniuses and super-intelligent proactive

geniuses globally, who are better than others, and better prepared to predict global future events

The Central Intelligence Agency (CIA's Good Judgments of the Future Predictors Project)

CONTINUE READING

INTELLIGENCE

The espionage war between China and the USA

Published 1 day ago on July 18, 2022
By **Dr.Nadia Helmy**

The intensity of US accusations of China of China's use of vast espionage networks behind Chinese intelligence to access information on the intellectual property of American inventions has increased. With the American assertion that Chinese espionage costs the United States of America more than $600 billion annually in stolen intellectual property. From here, you will find full cooperation and sharing of information between students, scholars, academics, and even Chinese citizens residing in the United States of America and all its various states with the "Chinese Ministry of National Security", and all official and national institutions of the Chinese state, and cooperation with Chinese security agencies, which are fully targeted regularly meeting with Chinese scholarship students abroad, especially in the United States of America.

Here, we find that one of the most prominent American fears is China's superior ability to

CONTINUE READING

INTELLIGENCE

India's Pakistan-bashing dossier

Published 3 days ago on July 16, 2022
By **Amjed Jaaved**

Since Pakistan announced that the Financial Action Task force was about to lift Pakistan from the “Grey List”, India was ill at ease. The dossier has tell-tale signs that it was a lame duck effort to compel the FATF to keep Pakistan at the Grey. Another stimulus for the production of the dossier was to do tit for tat to Pakistan’s dossier about India’s nefarious acts.

The dossier begins with rigmarole about the Jammu and Kashmir State which is a lingering dispute between India and Pakistan. India did not elaborate how it could unilaterally declare a disputed territory to be a part of the Indian Union.

The myth of accession

India is a signatory to the United Nations' resolutions on the disputed Kashmir state. By annexing it violated jus *cogen* of International Law, *pacta sunt servanda*. Treaties are binding on parties. Any country that flouts an international treaty qualifies as a rogue state and

CONTINUE READING

TRENDING

INTERNATIONAL LAW / 3 days ago

Regulate outer space before it is too late

RUSSIA / 3 days ago

Behind President Putin's visit to Iran

ENERGY / 4 days ago

The U.S. Government's Fake Opposition to Global Warming

AFRICA / 4 days ago

United Kingdom Pursuing Investment Projects in Africa

TERRORISM / 3 days ago

Analyzing link between Middle Eastern politics and the rise of ISIS

REPORTS / 4 days ago

World population to reach 8 billion this year, as growth rate slows

INTELLIGENCE / 3 days ago

India's Pakistan-bashing dossier

INTERNATIONAL LAW / 3 days ago

Endgame: Time, History and Alternative World Futures